CLAIMS

1. Traceable method for encrypting and/or decrypting data broadcast by at least one transmitter towards several decoders, this method enabling the identification of a traitor, amongst different lawful users of the decoders, who has communicated secret data to a non-authorized third party so that this third party is able to encrypt and/or decrypt data broadcast by the transmitter,

in which:

- during encryption of the broadcast data, the transmitter applies at least a first secret cryptographic function, and

- during decryption of said broadcast data, all the decoders apply at least one same second secret cryptographic function identical to said first function or its inverse, each decoder having recourse for this purpose to a mathematical description of said second function recorded in a memory,

characterized in that during the application of the second function the mathematical description of this second function, to which each decoder has recourse, is different from one decoder to another or from one group of decoders to another so that the mathematical description to which recourse is made exclusively identifies the particular decoder or group of decoders among all the decoders.

2. Method as in claim 1, characterized in that the second cryptographic function is able to process non-redundant data.

3. Method as in claim 1 or 2, characterized in that said mathematical description (F_{Kj}) recorded in the memory of each decoder is formed of several elementary functions ($G_{i,j}$) which must be composed with each other in a determined order to form said second secret function.

4. Method as in claim 3, characterized in that each elementary function ($G_{i,j}$) is equal to the composite of at least three functions as per one of the following equations:

$$G_{1,j} = f'_{1,j} \circ g_{\sigma j\,(1)} \circ S$$
$$G_{2,j} = f'_{2,j} \circ g_{\sigma j\,(2)} \circ f_{1,j}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$G_{r-1,j} = f'_{r-1,j} \circ g_{\sigma j\,(r-1)} \circ f_{r-2,j}$$
$$G_{r,j} = T \circ g_{\sigma j\,(r)} \circ f_{r-1,j}$$

in which:

- $G_{i,j}$ is the –th elementary function of decoder j, j being the index identifying a decoder or group of decoders,

- functions $f_{i,j}$ and $f'_{i,j}$ are predefined functions able to render the elementary functions $G_{i,j}$ non-commutative between each other,

- σ_j is a permutation of all indices {1; ...; r}unique to each decoder or group of decoders,

- $g_{\sigma j(t)}$ is the $\sigma_{j(t)}$ -th function of a predefined whole formed of r non-linear predefined functions g_i commutative between each other, and

- S and T are predefined functions able to render difficult the cryptanalysis of elementary functions $G_{1,j}$ and $G_{r,j}$ respectively,

5. Method as in claim 4 or 5, characterized in that each function f'_{ij} is equal to the inverse $f^{-1}_{i,j}$ of function $f_{i,j}$.

6. Method as in claim 4 or 5, characterized in that the functions $f_{i,j}$ are linear functions of a set (L^n) of the tuples of elements of a finished body (L) on itself.

7. Method as in any of claims 4 to 6, characterized in that the functions S and T are invertible.

8. Method as in any of claims 4 to 7, characterized in that the functions S and T are linear functions of a set (L^n) of the tuples of elements of a finished body (L) towards itself.

9. Method as in any of claims 4 to 8, characterized in that the functions g_i are chosen so that each elementary function $G_{i,j}$ corresponds to an encryption block of a multivariate encryption algorithm.

10. Method as in any of claims 4 to 9, characterized in that each function g_i is of the form $g_i(a) = a^{ei}$ in which a is an element of an L' extension of degree n of a basic body L with q elements, and e_i is a predefined exponent.

11. Method as in claim 10, characterized in that the exponent e_i is of the form : $1+q^{\theta 1} + \ldots + q^{\theta 1} + \ldots + q^{\theta d-1}$, in which the exponents θ_i are predefined integers.

12. Data recording medium, characterized in that it comprises instructions for the execution of a traceable encryption and/or decryption method according to any of the preceding claims, when these instructions are executed by a decoder.

13. Data recording medium, characterized in that it comprises instructions for the execution of a traceable data encryption and/or decryption method as in any of claims 1 to 10, when said instructions are executed by a transmitter.

14. Traceable system for encrypting and/or decrypting broadcast data capable of identifying a traitor, among different lawful users, who has communicated secret data to a non-authorized third party so that this third party is able to encrypt and/or decrypt the broadcast data, this system comprising:

- a transmitter able to encrypt broadcast data, this transmitter being capable of applying at least a first secret cryptographic function, to directly process a message, then of broadcasting the message,

- several decoders able to decrypt broadcast data, all the decoders being able to apply a second secret cryptographic function identical to said first function or to its inverse for the direct processing of said broadcast message, each decoder for this purpose being equipped with a memory in which a mathematical description of said second function is recorded;

characterized in that the memory of each decoder contains a mathematical description of said second function different from the one recorded in the memory of the other decoders or in the memory of the other groups of decoders so that this mathematical description exclusively identifies the particular decoder or group of decoders among all the decoders.

15. Memory intended to be associated with a decoder of a traceable data encryption and/or decryption system according to claim 13, characterized in that it comprises a mathematical description equivalent to said second secret function able to be used by the decoder, this mathematical description consisting of several elementary functions ($G_{i,j}$) each of which is equal to the composite of at least three functions as per one of the following equations:

$$G_{1,j} = f'_{1,j} \circ g_{\sigma j\,(1)} \circ S$$
$$G_{2,j} = f'_{2,j} \circ g_{\sigma j\,(2)} \circ f_{1,j}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$G_{r-1,j} = f'_{r-1,j} \circ g_{\sigma j\,(r-1)} \circ f_{r-2,j}$$
$$G_{r,j} = T \circ g_{\sigma j\,(r)} \circ f_{r-1,j}$$

in which:

- $G_{i,j}$ is the –th elementary function of decoder j, j being the index identifying a decoder or group of decoders,

- functions $f_{i,j}$ and $f'_{i,j}$ are predefined functions able to render the elementary functions $G_{i,j}$ non-commutative between each other,

- σ_j is a permutation of all indices {1; ...; r}unique to each decoder or group of decoders,

- $g_{\sigma j(t)}$ is the $\sigma_{j(t)}$ -th function of a predefined whole formed of r non-linear predefined functions g_i commutative between each other, and

- S and T are predefined functions able to render difficult the cryptanalysis of elementary functions $G_{i,j}$ and $G_{r,j}$ respectively.